1. Угроза безопасности информации. Базы данных угроз и уязвимостей.

2. Нарушитель в АС. Уровни возможностей. Вредоносное программное обеспечение.

3. Задача оценки угроз ИБ.

4. Показатели уязвимости информации.

5. Классификация и содержание угроз информации.

6. КНиГИ.

7. Методы и модели оценки уязвимости информации.

8. Модель уязвимости для несанкционированного копирования.

9. Математическое определение требований к защите информации.

10. Рекомендации по предъявлению требований к ЗИ. Рекомендации в зависимости от характера защищаемой И.

11. Рекомендации по предъявлению требований к ЗИ. Рекомендации в зависимости от объема и срока существования защищаемой И.

12. Рекомендации по предъявлению требований к ЗИ. Рекомендации для информации в терминалах пользователей и УГВВ.

13. Рекомендации по предъявлению требований к ЗИ. Рекомендации для информации в аппаратуре и линиях связи и центральном процессоре.

14. Рекомендации по предъявлению требований к ЗИ. Рекомендации для информации в ВЗУ и в хранилище носителей.

15. Рекомендации по предъявлению требований к ЗИ. Рекомендации для информации в устройствах подготовки данных и по территориальной распределенности.

16. Требования к защите информации, обуславливаемые видом защищаемой информации.

17. Специфические требования к защите информации на различных уровнях автоматизации.

18. Специфические требования к защите информации при взаимодействия АСОД и пользователя и этапами жизненного цикла АСОД.

19. Специфические требования к защите информации в зависимости от режимов функционирования АСОД. Общие рекомендации по формированию требований к ЗИ.

20. Показатели для оценки параметров защищаемой ИИ. ИИ как ресурс.

21. Показатели для оценки параметров защищаемой ИИ. ИИ как объект.

22. Оценка важности ИИ.

23. Оценка полноты ИИ.

24. Оценка релевантности ИИ.

25. Оценка адекватности ИИ.

26. Оценка толерантности, эффективности кодирования и объема И.

27. Определение и анализ понятий функций и задач защиты.

28. Методы формирования функций защиты.

29. Полное множество функций защиты.

30. Общая модель исходов при осуществления функций обеспечения ЗИ.

31. Зависимость уровня осуществления функций защиты от количества ресурсов.

32. Служба компьютерной безопасности. Состав, задачи, функции.

33. Служба компьютерной безопасности. Организационно-правовой статус, права.

34. Функции непосредственной защиты информации.

35. Разграничение прав доступа к ИИ.

36. Субъектно-объектная модель. Субъект, объект, пользователь.

37. Субъектно-объектная модель. Источник, ассоциации.

38. Субъектно-объектная модель. Доступ, правила.

39. Монитор безопасности. Аксиомы, обязательные требования.

40. Монитор безопасности. Следствия.

41. Политики доступа.

42. Общий критерий безопасности ИС (КС).

43. МБО, МБС.

44. Условия неизменности субъектов. Достаточное условие гарантий безопасности 1.

45. Замкнутость и изолированность. Достаточное условие гарантий безопасности 2.

46. Порождение субъектов. Базовая теорема НПО.

47. Модели дискреционного доступа. Адепт-50.

48. Пространство Хартсона.

49. Модель Харрисона-Руззо-Ульмана.

50. Модели мандатного уровня и специализированные модели.

51. Модель Белла-Лападула.

52. Критика модели Белла-Лападула.

53. Модель MTS.

54. Информационные модели. Модель невмешательства.

55. Информационные модели. Модель невыводимости.

56. Вероятностные модели. Игровая модель. Модель с полным перекрытием.

57. Модели контроля целостности. Модель Биба.

58. Модели контроля целостности. Модель понижения уровня субъекта.

59. Модели контроля целостности. Модель понижения уровня объекта.

60. Объединение моделей безопасности. Модель Боба.

61. Модель Кларка-Вилсона. Исходные данные.

62. Модель Кларка-Вилсона. Правила.

63. Отказ в обслуживании. Понятия.

64. Отказ в обслуживании. Требования.

65. Мандатная модель ОВО.

66. Модель распределения ресурсов Миллена.

67. Концепции осуществления функций управления ЗИ.

68. Репрезентативное множество задач ЗИ как классы.

69. Условия, повышающие эффективность ЗИ.

70. Идентификация и аутентификация.

71. Стойкость парольных систем.

72. Биометрическая идентификация и аутентификация.

73. Аутентификация на основе сертификатов.

74. Процедура рукопожатия.

75. Протокол Диффи-Хеллмана.

76. Экспертные оценки. Методы.

77. Коэффициент конкордации.

78. Коэффициент вариации.

79. АС. Защита от НСД. Понятия, классы, разница между классами.

80. СВТ. Защита от НСД. Понятия, классы, разница между классами.

81. СВТ. МЭ. Защита от НСД. Понятия, классы, разница между классами.

82. Хэш-функция. Семейство SHA. История разработки, особенности, применение.

83. Хэш-функция. Семейство MD5. История разработки, особенности, применение.

84. Стрибог. История разработки, особенности, применение.